This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-27 (cancelled).

28. (Currently Amended) A method for clustered Secure Sockets Layer (SSL) acceleration, comprising the steps of:

connecting at least two SSL relays in a cluster;

establishing a communication path between a first node and a second node via a first SSL relay of the cluster;

transferring information between the first node and the first SSL relay, the transferred information related to a communication from the first node to ~~a~~ the second node;

transferring the information between the first SSL relay and the second node;

receiving an acknowledgement from the second node in response to determining that the transferred information is a full record; and

clustering state information of the communication path in response to receiving ~~an~~ the acknowledgment from the second node ~~confirming receipt of the communication~~, the clustering comprising sharing the state information between the first SSL relay and at least a second SSL relay of the ~~relay~~ cluster, wherein the second SSL relay is capable of taking over communications between the first and second nodes upon failure of the first SSL relay.

29. (Previously Presented) The method according to claim 28, wherein the first node comprises a client and the second node comprises a server.

30. (Currently Amended) The method according to claim 28, further comprising transferring the information associated with the communications between the first node and the second node to the second SSL relay transparently upon failure of the first SSL relay.

31. (Previously Presented) The method according to claim 28, further comprising transmitting the communication from the first node to the second SSL relay and from the second SSL relay to the second node transparently upon failure of the first SSL relay.

32. (Cancelled).

33. (Cancelled).

34. (Previously Presented) The method according to claim 28, further comprising sharing an SSL session cache across all of the at least two SSL relays.

35. (Previously Presented) The method according to claim 28, further comprising clustering an SSL session resumption between the first node and the first SSL relay.

36. (Previously Presented) The method according to claim 28, further comprising clustering cryptographic keying information across all of the at least two SSL relays.

37. (Previously Presented) The method according to claim 36, further comprising clustering a key and a current Cipher Block Chaining (CBC) residue.

38. (Previously Presented) The method according to claim 36, further comprising clustering a sequence number.

39. (Previously Presented) The method according to claim 36, further comprising clustering a current key schedule.

40. (Previously Presented) The method according to claim 36, further comprising clustering a key and an offset into a key stream.

41. (Previously Presented) The method according to claim 28, further comprising clustering a cipher state.

42. (Previously Presented) The method according to claim 28, further comprising clustering data from a partial record corresponding to data from either the first or second node.

43. (Currently Amended) The method according to claim 28, further comprising clustering an ~~record~~ information size before the ~~record~~ information is transmitted.

44. (Currently Amended) A system for clustered Secure Sockets Layer (SSL) acceleration comprising:

a first node;

a second node; and

an SSL relay cluster for connecting the first node and the second node comprising:

a first SSL relay configured to cluster state information in response to ~~a first acknowledgment from the second node confirming receipt of data transmitted from the first node~~receiving a client handshake from the first node; and

a second SSL relay configured to transmit an ~~second~~ acknowledgment to the first SSL relay upon receiving the state information,

wherein the first SSL relay is further configured to transmit a handshake acknowledgment message to the first node upon receiving the acknowledgment from the second SSL relay.

45. (Previously Presented) The system according to claim 44, wherein the first node comprises a client and the second node comprises a server.

46. (Currently Amended) A computer readable medium storing computer readable instructions that, when executed by a processor, performs a method comprising:

establishing a connection between a first node and a second node via a first SSL relay of an SSL relay cluster, wherein said SSL relay cluster comprises at least two interconnected SSL relays;

receiving a data communication from the first node;

transmitting the data communication to the second node;

receiving a first acknowledgment from the second node ~~confirming receipt of the data communication~~in response to a determination that the transmitted data communication is a full record;

in response to the first acknowledgment, clustering state information of the established connection with at least a second SSL relay of the SSL relay cluster; and

receiving a second acknowledgment from the at least ~~the~~ second SSL relay in the SSL relay cluster confirming successful clustering.~~; and~~

~~in response to the second acknowledgment, transmitting a third acknowledgment to the first node~~.

47. (Currently Amended) The ~~apparatus~~ computer readable medium according to claim 46, wherein the second SSL relay assumes the first SSL relay's responsibilities upon failure of the first SSL relay.

48. (Currently Amended) The computer readable medium~~apparatus~~ according to claim 46, wherein the first node comprises a client and the second node comprises a server.

49. (Currently Amended) An SSL relay, the SSL relay connected in a cluster of SSL relays, comprising:

a first interface for transferring information between a first node and the SSL relay;

a second interface for transferring the information between a second node and the SSL relay;

a third interface for transferring state information between SSL relays in the cluster only in response to an acknowledgment from the second node, wherein the acknowledgment is

received in response to a determination that the transferred information is a full record ~~confirming receipt of transferred information~~; and

a storage device, wherein ~~the~~ state information of an SSL connection between the first node and the SSL relay is shared across each SSL relay in the cluster, any of the SSL relays in the cluster capable of taking over all connections of another SSL relay in the cluster, wherein the storage device is further configured to store the transferred information in a queue until acknowledgement is received from the second node. ~~therefore providing no interruption in the transfer of information should any of the SSL relays in the cluster fail~~.

50. (Previously Presented) The apparatus according to claim 49, wherein the first node is a client and the second node is a server.

51. (Previously Presented) The apparatus according to claim 49, wherein the first interface and the second interface are the same.

52. (Previously Presented) The apparatus according to claim 49, wherein the second interface and the third interface are the same.

53. (Previously Presented) The apparatus according to claim 49, wherein the first interface and the third interface are the same.

54. (Previously Presented) The apparatus according to claim 49, wherein the first interface and the second interface and the third interface are the same.

55. (New) The method of claim 28, further including the steps of:

clustering the transferred information in response to determining that the transferred information is a partial record; and

transmitting a partial acknowledgment to the first node upon clustering the transferred information.

56. (New) The method of claim 55, wherein the step of determining that transferred information is a partial record includes determining whether a packet interval timer has expired.

57. (New) The method of claim 28, further including the step of storing the transferred information in a queue until the information has been acknowledged by the second node.

58. (New) The method of claim 57, wherein the transferred information is stored in the queue with a cipher state associated with the information.

59. (New) The system of claim 44, wherein the state information includes at least one of: a client random value, a server random value and a chosen cipher suite.

60. (New) The system of claim 44, wherein the handshake acknowledgement message includes at least one of a server handshake and a server handshake completion message.

61. (New) The system of claim 60, wherein the first node is configured to transmit a key exchange message upon receiving the server handshake completion message.

62. (New) The computer readable medium of claim 46, further including the steps of:

clustering the data communication in response to determining that the data communication is a partial record; and

transmitting a partial acknowledgment to the first node upon clustering the data communication.

63. (New) The computer readable medium of claim 62, wherein the step of determining that the data communication is a partial record includes determining whether a packet interval timer has expired.

64. (New) The computer readable medium of claim 46, further including the step of storing the data communication in a queue until the data communication has been acknowledged by the second node.

65. (New) The computer readable medium of claim 64, wherein the data communication is stored in the queue with a cipher state associated with the record.